Electronic Banking Conditions

General Part

1 Our Obligations

We agree to grant access and make the electronic service available to you subject to and governed by the EBCs.

2 Your Obligations

2.1 You represent and warrant to us each time you use the electronic service, that:

(a) you have all necessary power, authority and approvals to enter into and perform your obligations under the EBCs;

(b) the EBCs and each instruction are your legally binding obligations; and

(c) your entering into and performance of the EBCs and each instruction does not violate, breach, conflict with or constitute a default under any law, regulation, rule, judgement, contract or other instrument binding on you or any of your assets or any provision of your constitutional documents.

2.2 You accept full responsibility for monitoring all information, records, transaction history and transactions available to you through the electronic service. You agree to notify us immediately if you become aware of any inaccurate information or unauthorised or incorrectly executed payment transactions. You agree that we will not be liable for any loss whatsoever if you fail to notify us of any such inaccurate information within 45 days of the date your account was debited or credited.

2.3 You agree to comply with all procedures and requirements as set out in the user manual(s) when using the electronic service. You also agree not to disclose the contents of the user manual(s) to any third party.

2.4 You agree that all intellectual property rights in the electronic service are and remain with us. Accordingly, you agree to undertake any and all actions, at our cost, that we may request to ensure our right title and interest in and to such intellectual property rights.

3 Use of the Electronic Banking Service

You agree to be responsible for ensuring that you fully comply with the local laws applicable to any access and use of the electronic service. You agree to indemnify us for any loss whatsoever which we may incur or suffer as a result of any claim against us arising out of your access and/or use of the electronic service unless caused by our gross negligence or wilful misconduct.

4 Instructions

4.1 You agree that we may rely and act upon all instructions given by you and you will be bound by any agreement entered into with us and liable for any loss incurred by us in relying on such instructions. You agree to indemnify us for any such loss.

4.2 We can refuse to act upon an instruction and take any action we deem appropriate in the circumstances, including cancelling or blocking your rights of access to the electronic service, if we have reasonable grounds to believe that it was not given by you;

(a) The instruction was not authorised by you;

(b) The instruction was not clear or you provided an incorrect unique identifier;

(c) Acting on the instruction will prevent us complying with what we consider to be our obligations under applicable law, regulation or guidelines of a regulatory authority;

(d) Acting on the instruction might cause us to breach a contractual duty or prevent our complying with our obligations under any contract;

(e) Your rights of access to the electronic services are being used for an unlawful purpose, including, but not limited to, a violation of sanctions legislation, anti-money laundering or terrorism financing legislation; or

(f) There has been, or we have reason to believe there is about to be, an unauthorised disclosure of your security details or other security breach or a breach of these EBCs generally.

If we refuse to act upon an instruction, we will inform you, as soon as reasonably practicable, that the instruction has not been acted upon by us. We may charge you for such notification. If we block your access to the electronic service, we will inform you before doing so, if possible, and, if not, immediately thereafter. If possible and as long as not prohibited by other laws or regulation, we will provide you with the reasons for our refusal to act or our blocking of access.

4.3 You must ensure that all instructions from you to us are clear and accurate. You must also follow any procedures for submitting instructions that we may provide to you, whether electronically, by post or by hand

4.4 The instructions from you will be deemed received by us on the banking day when received if they are received before the applicable cut-off time or at such other time as we have agreed upon, as long as this is a banking day. The applicable cut-off time will be communicated by us to you from time to time. If the instructions are received after the cut-off time or on a day that is not a banking day, the instruction will be deemed to have been received on the next banking day.

4.5 In acting upon your instructions, we shall rely exclusively on the unique identifier provided by you in the instructions. If we act on an incorrect unique identifier provided by you, we will make

reasonable efforts to recover the funds involved but will not be liable to you for any loss if we are unable to do so.

4.6 If you revoke an instruction after we have received it or after close of business on the banking day previous to the day agreed for the execution of the instruction, we will make reasonable efforts to cancel the instruction but will not be liable to you if we are unable to do so.

4.7 We may record instructions in order to ensure we have a full record of all instructions received by us. You agree and consent to us monitoring the electronic service in order to help us improve the quality of our service to you.

4.8 You agree that our records and statements as to dates, amounts or rates shall, in absence of manifest error, be conclusive evidence of the facts reflected in those records or statements.

5 Security

5.1 You must comply with all security procedures provided by us to you whether supplied electronically, by post or by hand, including, where relevant, those set out in the user manual(s). In addition, you must take all reasonable precautions to prevent a security breach.

5.2 You must contact us immediately by telephone (and shall confirm the telephone call by giving us written notice within forty eight hours of such call) if you have grounds to suspect any security breach. You will be responsible for any instruction that was not given by you upon which we have acted in good faith and in circumstances where we complied with security procedures provided to you in writing, including security procedures set out in the user manual(s).

5.3 Where you have informed us that an instruction was not given by you and is to be cancelled, you will not be responsible for that instruction if we have not acted upon it and are able to cancel it by using our reasonable endeavours to do so.

5.4 You must use your best efforts to comply with our instructions on steps to remedy any security breach, including but not limited to providing us with information which we may reasonably request relating to your use of the electronic service and co–operating with us in any related investigation.

6 Liability and Indemnity

6.1 We will not be liable for any loss incurred by you in connection with the electronic service, including but not limited to any security breach, unless caused by our gross negligence or wilful misconduct. In no circumstances will we be liable for any consequential, indirect, economic, special or punitive losses.

6.2 We will not be liable to you for any loss whatsoever if we do not act upon your instructions or are prevented from providing the electronic service because of any cause that we cannot reasonably control, including but not limited to:

(a) the unavailability of any communication network or any other communication system (including, without limitation, the internet) or data becoming scrambled, lost in transmission or wrongly communicated due to any reason whatsoever including defects in any communication network, or direct or indirect failure of power supplies, equipment, data processing and communication systems or transmission links;

(b) the failure of any settlement system chosen by you or us;

(c) circumstances where we are prevented from providing the electronic service because of a strike or other industrial action; or

(d) any other circumstances that are abnormal or unforeseeable, the consequences of which are unavoidable despite all efforts to the contrary.

6.3 You agree to indemnify us and keep us indemnified from and against any and all losses resulting from acts or omissions to act by you or any of your authorised representatives under the EBCs, including, but not limited to, any breach of the EBCs, any violation by you of our rights, your violation of any applicable law, any failure to prevent a security breach or mitigate the effects of such a breach, and any third party claim arising out of or relating to your use of, or failure to use, our electronic service, unless these losses are caused by our gross negligence or wilful misconduct.

7 Charges and Taxes

7.1 You agree to pay us fees and charges (together with all applicable taxes) as agreed in writing between you and us from time to time. For the avoidance of doubt, all goods and services tax, value–added taxes or other similar taxes due in respect of any sums payable under the EBCs will be paid by you. In addition, we may charge you for any measures required to be undertaken by us that are of a corrective or preventive nature, including but not limited to any efforts undertaken pursuant to clauses 4.5 and 4.6.

7.2 Any such amounts due from you may be deducted by us from any funds in the account(s) held with us. You agree that we may also deduct any charges due to us from funds that are transferred to you, prior to crediting your account with these funds.

8 Changes to EBCs

8.1 We can change and supplement the EBCs, and/or suspend or discontinue any aspect of our electronic service at any time in order to take into consideration a material development in our business, the introduction of new products and services or to reflect a change of law. If we do so, we will endeavour to provide you with at least 30 days' prior notice of any such change or addition to the EBCs, unless this is not reasonably practicable in the circumstances. All such changes and additions will be binding on you and us.

8.2 Amendments to reflect a change of law may take effect immediately. Other amendments will take effect on the date notified to you.

9 Notices

9.1 Any notice to you under these EBCs can be given by electronic mail, prepaid post or courier to the address you have provided to us in the licence form.

9.2 If sent by electronic mail to you, any notice will be deemed delivered when received in your electronic mail box. If sent by

prepaid post or courier, any notice will be deemed delivered on actual receipt.

9.3 Any notice from us will be deemed to be given as follows:

(a) if by letter, when left at the recipient's address, on the day it was so left, or, if sent by post, two business days after the time when the same was put in the post and in proving delivery it shall be sufficient to prove that the same was properly addressed and put in the post;

(b) if by telex, when despatched, but only if, at the time of transmission, the correct answerback appears at the start and at the end of the sender's copy of the notice;

(c) if by facsimile, when a positive transmission report is received by the Bank;

(d) if by telephone, when audibly heard by the receiver of the Communication; and

(e) if by electronic banking arrangement or electronic mail, when received in comprehensible form by the receiver of the Communication in its electronic mail box.

10 Assignment

Neither party may transfer or assign its rights, benefits and or obligations under the EBCs without the prior written consent of the other party.

Notwithstanding this you acknowledge and agree that:

(a) we may, at any time and in our entire discretion, assign any of our rights or transfer by novation or otherwise any of our rights and obligations under the EBCs and any agreement with you which incorporates the EBCs by reference (the "Relevant Agreement") (the "Transfer") to any of the subsidiaries or affiliates of The Royal Bank of Scotland Group plc (the "Transferee"), without your further consent;

(b) the Transfer will take effect from the date specified in a notice in writing from us to you;

(c) in the case of a transfer by novation, from the effective date of the Transfer:

(i) you and we shall be released from further obligations to one another under the Relevant Agreement your respective rights against one another under the Relevant Agreement are to be cancelled (being the "Discharged Rights and Obligations");

(ii) you and the Transferee shall assume obligations towards one another and/or acquire rights against one another which differ from the Discharged Rights and Obligations only insofar as you and the Transferee assume and/or acquire the same in place of you and us; and

(iii) all references to "us" and "we" and other related references in the EBCs are to be read and construed as references to "the Transferee" with other contextual changes made as required; and

(iv) you will do all things required by the Transferee to give full effect to the Transfer and to the Relevant Agreement including, but not limited to, executing any document and performing any act.

Without prejudice to the above, you further agree that we have the right, without your consent, to assign any of our rights and transfer any of our obligations to any of our affiliates.

11 Confidentiality and Use of Information

11.1 We will not communicate your confidential information to third parties without your consent unless:

(a) we are required to do so by law or regulation; or

(b) we are permitted to do so by law including, but not limited to, disclosure for the purposes of any legal proceedings.

11.2 In addition to the disclosures in clause 11.1, you agree that we may disclose your confidential information to:

(a) any of our affiliates, including, but not limited to, affiliates where the technical processing of data is located and centralised;

(b) any of our professional advisers;

(c) credit agencies (for the purpose of our credit rating); or

(d) any third party to the extent it is involved in providing the electronic services used by you or to the extent such third party is necessary to the provision of these electronic services to you.

We will use our reasonable endeavours to advise the other parties to whom we disclose your confidential information under this clause of the confidential nature of such information.

11.3 We may disclose information received from you about your employees or authorised representatives to any of our affiliates, agents and subcontractors for operational or other legitimate business purposes. You agree that we may transfer such information to our affiliates, agents and subcontractors who conduct their business from countries outside the European Union. You also agree that we may transfer such information to our electronic server in the European Union, or electronic servers within the European Union provided by our service providers or subcontractors. Some of such countries may not necessarily have data protection laws providing safeguards as strong as those within the European Union. You agree to inform your authorised representatives of these facts on our behalf.

12 Termination

12.1 Either party may terminate the EBCs or any specific electronic service or product at any time by giving notice to the other, which termination will take effect after a period of 30 days or such longer period as may be specified in the notice.

12.2 Either party may terminate the EBCs immediately by giving notice to the other if:

(a) it has reasonable grounds to believe that there has been a serious or persistent breach of the EBCs by the other party;

(b) the other party is unable or admits its inability to pay its debts as they fall due or becomes (voluntarily or involuntarily) the subject of any proceedings under any relevant liquidation, bankruptcy, winding–up, reorganisation (save for solvent reorganisation), judicial management or similar law; or

(c) the other party becomes aware of circumstances which are likely to give rise to any of the events in (b) above.

12.3 Termination will only have future effect and will not affect any outstanding transactions, rights or obligations. Unless we have terminated the EBCs because of a serious or persistent breach of the EBCs by you, we will refund the proportion of any fee or charge paid by you in advance which falls beyond the date of termination. Both parties agree that clauses 6 and 11 will continue in force if the EBCs are terminated.

13 General Terms

13.1 If any provision of these EBCs is held to be invalid or ineffective, it will not affect any other provisions of the EBCs.

13.2 No failure or delay on the part of either party to exercise any right or remedy under these EBCs will operate as a waiver of such right or remedy.

13.3 The electronic services may be provided using the services of our affiliates, agents or third party sub–contractors. You agree that such third party service providers are third party beneficiaries of the provisions of the EBCs which apply to us, including provisions which indemnify us or limit our liability.

13.4 In the event of any conflict between the provisions of the EBCs and the provisions of the applicable schedules, the provisions of the schedules will prevail.

13.5 Other than as provided in clause 13.3, a person who is not a party to the EBCs will not have any rights under the EBCs or any applicable statute (if any) unless we give our written agreement to that person having such rights.

14 Meaning of Words

account means any account(s) held by you or any third party with us or any third party bank and for which you have agreed with us that the electronic service is to be made available;

affiliate means any related company, partnership, branch or other form of business;

authorised representative means your employee (or any third party) authorised by you to operate the electronic service;

banking day means any day on which:

(i) banks in the relevant jurisdiction where our services are provided are generally open for business and as required for the execution of a payment transaction, other than weekends and local bank holidays; and

(ii) the relevant settlement system is open to settle your instruction;

communication network means any of the communication systems and networks set out in the schedules;

confidential information means any information that we obtain about you in connection with providing the electronic service to you (including any information about any account) other than information which is or becomes publicly available;

EBCs and Electronic Banking Terms and Conditions means these Electronic Banking Terms and Conditions, the applicable schedules for the services and products selected by you in the licence form (s) signed by you, the user manual(s), and the security procedures we have provided to you with the EBCs

electronic service means our electronic services and products set out in the schedules and selected by you in the licence form;

electronic signature means data in electronic form which is attached to or logically associated with an instruction or other electronic data and which serves to authenticate such instruction or data;

instruction means an instruction that (i) has been verified by security details; (ii) includes your consent to our acting upon it; and (iii) has been made through a communication network/Internet to us, and which is conducted through the electronic service;

intellectual property rights means any patents, trademarks, service marks, design rights, copyrights, know–how, database rights, trade or business names and other similar rights or obligations and including all applications for and all rights to apply for the same;

licence form means the document that you are required to complete and sign if you wish to use our electronic service;

letter of credit means documentary letters of credit and stand by letters of credit;

loss means damages, costs, expenses, loss or liability or claim;

payment instrument means any personalised device(s) and/or set of procedures agreed between you and us and used by you to initiate a payment transaction;

schedules means those schedules from time to time attached to these EBCs which set out our products and services and the relevant communication network;

security breach means any violation of the security procedures described in the EBCs and/or the user manual(s), including but not limited to the unauthorised disclosure of the security details or the fraudulent or unauthorised use of access to your security details or the electronic service;

security details means either an electronic signature or other information established between us which enables us to verify your identity or the identity of your authorised representative;

software means any computer programs provided by us to you in order to use the electronic service;

unique identifier means the combination of letters, numbers or symbols specified from time to time to you by us (e.g. the beneficiary's account number and sort code) to be provided by you to identify unambiguously the beneficiary to the payment order given to us by you or the beneficiaries' payment account;

user manual means the manual (if any) as may be amended from time to time which we provide to you whether electronically, by post or by hand and which contains information, procedures and requirements about the electronic service;

we means the subsidiary or affiliate of The Royal Bank of Scotland Group plc specified in the Electronic Services Licence Form and its successors and **our** and **us** shall be construed accordingly; and

you means the customer who has accepted the EBCs, and your shall be construed accordingly.

Words employing the singular include the plural and vice versa.

15 Jurisdiction

15.1 The EBCs are governed by the law of country that has been agreed between you and us.

15.2 The courts of country that has been agreed between you and us will have exclusive jurisdiction over all disputes arising in connection with the EBCs and each party irrevocably waives any objection it may have at any time to the jurisdiction of such courts. This exclusive clause is for our benefit, and so notwithstanding the reference to exclusive jurisdiction we can also pursue our remedies in the courts of any other appropriate jurisdiction.

16 Country specific changes

16.1 The EBCs that are agreed between you and us may contain country specific elements that are not included in these general terms & conditions.

Schedule – Access Online

1. Access Online

Access Online is an integrated, single sign–on environment that will enable you to access a range of **dynamically linked** products and services from our diverse business functions including:

(a) Global Cash Management (Online Payments and Balance & Transaction Reporting);

(b) Financial Markets (Access Online FX);

(c) Trade (MaxTrad and MaxTrad Express); and

(d) Liquidity Management.

To the extent you have agreed that we will deliver these products and services you will find a more detailed description of each of the products and services in the Online Channel Schedules and in each of the available product user manuals.

2. Equipment

You are responsible for ensuring the compatibility of your Internet browser, its setting and any of your equipment with Access Online.

Schedule – Access Online – Global Cash Management

1. Access Online – Global Cash Management

Access Online – Global Cash Management as further described in the user manuals will enable you to:

(a) obtain information, including information on balances and transactions from the accounts;

(b) transfer funds to and from the accounts;

(c) generate bank cheques from the accounts;

(d) deliver and receive information between us;

(e) send online service requests;

(f) view on screen images of cheques collected by us on your behalf; and

(g) do any other transaction as we may permit under Access Online – Global Cash Management from time to time.

2. Equipment

You are responsible for ensuring the compatibility of your internet browser, its settings and any of your equipment with Access Online – Global Cash Management.

Schedule – Access Online – Global Cash Management – Balance and Transaction Reporting and User Administration modules

1. Access Online – Global Cash Management – Balance and Transaction Reporting and User Administration modules

The Access Online – Global Cash Management – Balance and Transaction Reporting and User Administration modules, as further described in the user manuals will enable you to:

(a) obtain information, including information on balances and transactions from the accounts;

(b) deliver and receive information between us;

(c) send online service requests;

(d) view on screen images of cheques collected by us on your behalf; and

(e) do any other transaction as we may permit under the Access Online – Global Cash Management – Balance and Transaction Reporting and User Administration modules from time to time.

2. Equipment

You are responsible for ensuring the compatibility of your internet browser, its settings and any of your equipment with the Access Online – Global Cash Management – Balance and Transaction Reporting and User Administration modules.

Schedule – Access Online – Global Cash Management – Payments module

1. Access Online – Global Cash Management – Payments module

The Access Online – Global Cash Management – Payments module as further described in the user manuals will enable you to:

(a) obtain information, including information on payments initiated from the accounts via Internet;

(b) transfer funds to and from the accounts;

(c) generate bank cheques from the accounts;

(i) deliver and receive information between us;

(j) view on screen images of cheques collected by us on your behalf; and

(d) do any other transaction as we may permit under the Access Online – Global Cash Management – Payments module from time to time.

2. Equipment

You are responsible for ensuring the compatibility of your internet browser, its settings and any of your equipment with Access Online – Global Cash Management – Payments module.

Schedule – Access Online – Liquidity Management and Liquidity Solutions

1. Access Online – Liquidity Management and Liquidity Solutions

Access Online – Liquidity Management and Liquidity Solutions as further described in the user manuals will enable you to:

(a) Obtain information, including information on balances and transactions from the accounts including investment accounts;

(b) Transfer funds to and from the accounts;

(c) Deliver and receive information between us;

(d) Send online service requests;

(e) Change Multi Bank Cash Concentration settings and other cash pooling product settings as may be permitted by us. You are responsible for any changes you make to those settings [in particular (i) if you change the time of a payment it is your responsibility to ensure it meets the applicable cut-off time (otherwise the instruction will be deemed to have been received on the next banking day) (ii) if you make a change to the payment type, this may affect the applicable cut-off time]; and

(f) do any other transaction as we may permit under Access Online – Liquidity Management and/or Liquidity Solutions from time to time.

2. Equipment

You are responsible for ensuring the compatibility of your internet browser, its settings and any of your equipment with Access Online – Liquidity Management and Liquidity Solutions.

Access Online – Security Procedures

Words defined in our Electronic Banking Terms and Conditions shall have the same meaning when used in these security procedures

1. Access Setup Form

1.1 Prior to your installation of Access Online, you must complete and deliver to us the Access Setup Form (ASF). You will specify on the ASF one or more users who will be designated as security managers and one or more users who will be designated as administrators for Access Online.

1.2 The designated security manager(s) and administrator(s) will perform separate tasks as outlined below.

1.3 We recommend that different individuals be designated for these critical positions. We will presume that the security manager and the administrator have the authority and responsibilities identified below unless otherwise agreed in writing.

2. Roles of administrator and security manager

2.1 We recommend that the authority and responsibilities of the **security manager** include:

(a) Acting as the main contact person for us with regards to the implementation and delivery of Digipass or bankcard token based services; and

(b) Requesting via the ASF, or through an online facility, issuance of Digipass tokens or bankcard tokens for employees within the company.

2.2 We recommend that the authority and responsibilities of the **administrator** include:

(a) Creation of individual user privileges; creation of user account privileges accounts which users can debit; and creation of the authorisation matrix used to set up authorisation limits for each user for Access Online as described in the user manual;

(b) Supervising the maintenance of the separation of functions

(c) Verifying user activity at regular intervals and making sure that they reflect accurately the actual authorisation levels intended within the organisation; and

(d) Checking audit trails to ensure that all actions are carried out correctly by the appropriate users and reporting any deviations to management.

3. Online User Administration (OUA)

3.1 Administrators use OUA to instruct us to create new users, temporarily or permanently suspend users, assign or change user profiles and roles and user account privileges and set up and change the authorisation matrix. In signing the ASF, the legal representatives of your company empower the administrator to carry out these changes electronically with full legal force, as if the legal representatives had authorised these changes on an executed paper form.

3.2 If your company indicates preference for OUA with Dual Control on the ASF, a designated authoriser must authorise all instructions that administrators enter. The authoriser role is indicated on the ASF or is assigned by an administrator using OUA.

3.3 In OUA, administrators set up and maintain the authorisation matrix, which defines authorisation rights for each user according to account, amount, payment type and various other criteria. The authorisation matrix also defines if a payment must be authorised by more than one user, and if so by which combination(s) of users, in order for us to accept it for processing.

3.4 By assigning roles to users in OUA, administrators set up and maintain function access control, which restricts access to menu functions.

3.5 By creating and assigning Data Access Profiles (DAPs) to users in OUA, administrators set up and maintain data access control, which restricts access to certain accounts, beneficiaries or other data.

3.6 We create the initial set–up of administrators, authorisers, their rights and roles, and the authorisation matrix based on the set–up agreed to on the ASF. Thereafter administrators maintain the set–up as indicated above. Only if your company only has one administrator, we will maintain the administrator's user profile and rights. In that case changes must be requested using a ASF signed by the company's legal representatives.

4. Access Online password format

4.1 Unless using a bankcard token, authorised users can access Balance and Transaction Reporting, RFQ and Trade Services either by

(a) entering their username and password, or

(b) by both entering username and providing an electronic signature using a Digipass.

4.2 Logon to the Online Payments module of Access Online and OUA requires both entering username and providing an electronic signature using a Digipass.

4.3 All users, regardless of the applications that they access, must log on using username and password once every ninety days.

4.4 We will securely deliver the administrator's initial password to the designated administrator. The password is temporary and when first used the system will prompt the administrator to change it immediately.

4.5 Thereafter, the administrator assigns and resets user passwords, and if there is more than one administrator, the passwords of other administrators. If there is only one administrator, we must reset the password.

4.6 Access Online passwords must conform to the following password policy:

(a) Passwords should be between 6 and 32 characters long.

(b) Passwords are case–sensitive and should include at least one digit (0–9) and one character (a–z).

(c) Passwords may contain periods, commas, hyphens, etc.

(d) Passwords cannot contain more than 3 consecutive identical characters (e.g. 'aaaa' is not possible).

(e) Passwords cannot contain words from the user profile (e.g. user name, company, or city are not possible).

(f) Passwords will have to be changed at least every 90 days. Users will be notified seven days in advance.

(g) New passwords have to differ significantly from old passwords (a password history of twelve past passwords is retained).

4.7 All passwords are hashed (in other words, a “digital fingerprint” is created for each password).

4.8 A user has three attempts to enter the correct password, after which the user will be disabled and will require an administrator to unlock the account.

5. Authentication and electronic signatures using Digipass

5.1 Unless the bankcard and e.dentifier logon procedure applies, users must use a Digipass token and PIN code in order to authenticate their identity when logging on to various Access Online services. This is done as follows:

(a) The user enters his or her username in the logon screen;

(b) Access Online displays a six–digit challenge code onscreen;

(c) The user enters the six–digit challenge code on his or her Digipass, which generates a response code based on the challenge code;

(d) The user types the response code into the response box onscreen;

(e) Our server verifies whether the response code matches the username entered, and that the Digipass token used to generate the dynamic password is the Digipass assigned to that user; and

(f) If the response code is correct, the user is granted access to the Access Online service.

5.2 In various applications, users must use security instruments, such as a Digipass token and PIN code to generate an electronic signature, also known as a Message Authentication Code (MAC) to authorise and transmit instructions to us. The MAC is used to authenticate the sender of each instruction, and to protect the integrity of the each instruction while it is stored and processed within our systems. The MAC is created using an electronic key stored in a central security module and verified before processing takes place. This MAC implementation offers protection from tampering with the instruction since authentication would fail if even one character within the instruction were changed. The MAC is generated as follows:

(a) Access Online displays a eight–digit challenge code (also known as a “hash”) onscreen, based upon the data which the client is signing;

(b) The user enters the hash on his or her Digipass, which will generate a response code based on the hash;

(c) The user types the response code into the response box onscreen;

(d) Our server verifies whether the response code matches the username entered, and that the Digipass token used to generate the dynamic password is the Digipass assigned to that user; and

(e) If the response code is correct, the instruction is accepted for processing by us and the user is informed onscreen that the MAC was successful.

5.3 Digipass realises the authentication and MAC functions using the Triple DES algorithm.

5.4 Digipass PIN code format:

(a) The PIN code is a 4 character numeric code. The user has three attempts to enter the correct PIN code, after which the Digipass will be locked.

(b) Upon commencing use of the system the user will be prompted to change the initial PIN code issued by us. This represents a further security measure as now only the user has access to the PIN number.

5.5 Managing Digipass tokens and PIN codes:

(a) It is the responsibility of the security manager to deliver a Digipass to each authorised user. The Digipass will **only** be activated when we receive a notification of the delivery of the Digipass and PIN to the end–user by the security manager.

(b) Access to applications requiring a Digipass will **only** be activated when the administrator adds the Digipass ID to the user profile using OUA.

(c) Each Digipass, with its unique PIN code is intended for the exclusive personal use by the assigned user. Accordingly, a Digipass must not be transferred, loaned, or shared, even if the other person has been authorised to submit instructions to us. Within the organisation, the security manager administers users who is authorised to use Digipass token.

(d) The user must exercise due care with the Digipass and PIN code issued to him or her.

6. Authentication and electronic signatures using bankcard and e.dentifier

6.1 If the bankcard and e.dentifer logon procedure applies, users authenticate their identity when logging on to Access Online services as follows:

(a) The user enters his or her account– and cardnumber in the logon screen;

(b) Access Online displays an eight–digit challenge code onscreen;

(c) The user enters the eight–digit challenge code on his or her e.dentifier, which generates a six–digit response code based on the challenge code;

(d) The user types the six–digit response code into the response box onscreen;

(e) Our server verifies whether the response code matches the account– and cardnumber entered; and

(f) If the response code is correct, the user is granted access to Access Online or the Access Online service.

6.2 In various applications, users must use their bankcard and PIN code and an e.dentifier to generate an electronic signature, also known as a Message Authentication Code (MAC) to authorise and transmit instructions to us. The MAC is used to authenticate the sender of each instruction, and to protect the integrity of the each instruction while it is stored and processed within our systems. The MAC is created using an electronic key stored in a central security module and verified before processing takes place. This MAC implementation offers protection from tampering with the instruction since authentication would fail if even one character within the instruction were changed. The MAC is generated as follows:

(a) Access Online displays an eight–digit challenge code onscreen, based upon the data which the client is signing;

(b) The user enters the eight–digit challenge code on his or her e.dentifier, which will generate a six–digit response code based on the challenge code;

(c) The user types the six–digit response code into the response box onscreen;

(d) Our server verifies whether the response code matches the account– and cardnumber entered, and the specific instruction(s) from the user that need to be authorised by the MAC; and

(e) If the response code is correct, the instruction is accepted for processing by us and the user is informed onscreen that the MAC was successful.

6.3 If made in accordance with our instructions, a MAC will have the same consequences and legal effect as a written instruction signed by the user.

6.4 Bankcard PIN code format:

The PIN code is a 4 character numeric code. The user has three attempts to enter the correct PIN code, after which the bankcard will be blocked.

6.5 Managing bankcard and PIN codes:

(a) It is the responsibility of the security manager to deliver a bankcard with an undisclosed PIN code and an e.dentifier to each authorised user. The bankcard will **only** be activated when we receive a notification of the delivery of the bankcard, the undisclosed PIN code and the e.dentifier to the end–user by the security manager.

(b) Access to applications requiring a bankcard and PIN code will **only** be activated when the administrator adds the ID to the user profile using the User Administration module.

(c) Each bankcard, with its unique PIN code is intended for the exclusive personal use by the assigned user. Accordingly, a bankcard must not be transferred, loaned, or shared, even if the other person has been authorised to submit instructions to us. Within the organisation, the security manager administers users who are authorised to use bankcard tokens.

(d) The user must exercise due care with the bankcard and PIN code issued to him or her.

(e) The user or the security manager shall promptly notify us if a bankcard is lost, stolen, abused or counterfeited; the user or the security manager knows or suspects that a third party knows a PIN code; or the user or the security manager notices irregular circumstances.

(f) Further to clause 6 of the EBCs, we are not liable for damage caused, directly or indirectly, by the bankcard or the e.dentifier functioning improperly or not functioning at all.

7. Security during transmission

All data that Access Online transmits is encrypted using 128–bit Secure Socket Layer (SSL) encryption, which maintains the confidentiality and integrity of the data while communicated over the Internet. SSL protocol establishes the identity of the web site and encrypts the transmission channel between web browser and web site to keep transmitted information confidential. Only the user who establishes a secure web connection can see the data unencrypted. Any attempted change to the data will be detected and disallowed.

8. Security at client location

8.1 As a PC is considered a non–secure software environment you must apply the following additional security measures to enhance the integrity of this environment:

(a) Installing PC security software packages, including anti–virus software

(b) Regular updates of anti–virus software and other security related software, including the operating system and browser.

(c) Periodical deletion of unneeded security certificates, which may be configured in the installed browser by default.

(d) Changing your Access Online password every 90 days, unless the bankcard and e.dentifer logon procedure applies.

8.2 To further enhance PC security, all users must be instructed to adhere to the following guidelines:

(a) Passwords or PIN codes must never be revealed to others.

(b) PCs must never be left unattended when Access Online is running. A user leaving his or her desk for a short period must either exit the program, or use a password–protected screensaver.

9. Audit Trails

Access Online provides audit trails:

9.1 for the Online Payments module of Access Online, which log all user activities with regard to particular instructions.

9.2 for OUA, which record all administrative actions, including date, time, and user ID of administrators carrying out their tasks.

Schedule – Access Online – Central and Eastern Europe

1 Access Online – Central and Eastern Europe

1.1 Access Online – Central and Eastern Europe refers to the internet banking channel known as Access Online - Czech Republic, Access Online - Poland, or Access Online - Romania.

1.2 Access Online as further described in the user manual will enable you to:

(a) obtain information, including information on balances and transactions from the accounts;

(b) transfer funds to and from the accounts;

(c) set up collection orders (direct debits) to be made to the accounts;

(d) deliver and receive information between us; and

(e) do any other transaction as we may permit under Access Online from time to time.

2 Our Obligations

2.1 We will:

(a) provide access to an internet portal for Access Online; and

(b) provide training and support to you in relation to Access Online, if separately agreed between us and you.

3 Your Obligations

3.1 Where required by any law or directive of any state or organisation, you shall obtain all necessary consents, approvals, licences and permits from all authorised representatives, third parties, governmental agencies and regulatory authorities for any use or marketing of personal data and to the international transfer of personal data by us via the internet banking service.

3.2 You agree that at our reasonable request, you will provide us with copies of any such consent, approval, licence or permit.

4 Software Licence

4.1 In order to use Access Online, you are granted access to use the Access Online service on the following terms and conditions:

(a) you agree to only use the service for the purposes set out in section 1 above;

(b) you will treat the service as confidential;

(c) except with our consent, you will only use the service for your own business purposes and not for the purpose of providing services to any third party nor will you allow access or make the service available to any third party; and

(d) you will not do anything which would result in any infringement or unauthorised use of our or our suppliers' intellectual property rights in the service or the user manual.

4.2 For the avoidance of doubt, you will not acquire any title, ownership interest or intellectual property right in the service or the user manual.

4.3 We warrant that the service supplied by us to you provides in all material respects the functions set out in the user manual, provided it is properly used on the equipment and with the operating system and internet browser for which it was designed, as set out in the user manual. **So far as permitted by applicable law, we do not make any other warranty express or implied, statutory or otherwise, as to the condition, quality or performance or fitness for purpose of the service.**

4.4 We will indemnify you against any loss you incur as a result of any legal action based on an allegation that the service infringes any intellectual property right of any third party provided that you:

(a) promptly inform us in writing (in reasonable detail) of the existence of any such legal action;

(b) make no admission of liability;

(c) do not reach any settlement; and

(d) leave the handling of the case entirely to us. For this purpose you agree to execute all documentation we reasonably request and provide us with all information and co-operation required to defend any such action. You also consent to us retaining the benefit of any such litigation.

4.5 You will be responsible for maintaining the security of your data and ensuring that your data is adequately backed-up. We will not be liable to you for the loss of your data in any circumstances regardless of whether such data is also maintained by us.

5 Equipment specification

You are responsible for ensuring the compatibility of your internet browser, its settings and any of your equipment with Access Online.

6 Collection Orders (Direct Debits)

You agree to obtain all appropriate agreements before instructing us to set up any collection orders for payments to be made into your account. You agree that on our reasonable request you will provide us with copies of any such agreements.

7 Security

You will ensure that:

(a) all security instruments and security tokens are held securely by you;

(b) all security tokens are only issued by your security personnel to your authorised representatives;

(c) all PIN numbers and other passwords are known only to your authorised representatives and are never recorded in any written form; and

(d) all equipment is maintained in a suitably secure environment and is not left unattended while any third party is present.

Access Online – Central and Eastern Europe – Security Procedures

Words defined in our electronic terms and conditions shall have the same meaning when used in these Security procedures

1 Request for Information / Access Setup Form

1.1 Prior to providing you access to Access Online – Central and Eastern Europe (Access Online CEE), you must complete and deliver to us the Access Online CEE Request for Information (RFI) form. You will specify on the RFI one or more users who will be designated as security managers for Access Online CEE. Based on the RFI an Access Setup Form (ASF) will be created. This ASF needs to be signed before access is granted.

1.2 The designated security manager(s) will perform separate tasks as outlined below.

1.3 We will presume that the security manager has the authority and responsibilities identified below unless otherwise agreed in writing.

2 Role of security manager

2.1 We recommend that the authority and responsibilities of the **security manager** include:

(a) Acting as the main contact person for us with regards to the implementation and delivery of Digipass based services; and

(b) Requesting, via the RFI/ASF, the issuance of Digipass tokens for employees within the company.

(c) Requesting via a RFI/ASF creation of individual user rights; defining of user account privileges. Defining accounts which users can debit; and defining the authorisation matrix used to set up authorisation limits for each user for Access Online CEE as described in the RFI/ASF;

(d) Supervising the maintenance of the separation of functions

3 Authentication and authorisation

3.1

(a) Authorised users can access Access Online CEE by either entering their username and password, or (if applicable) or

(b) by entering username and providing an electronic signature using a Digipass.

3.2 Creation of payment orders in Access Online CEE always requires entering username and providing an electronic signature using a Digipass.

3.3 All users, that have been granted access with a password, regardless of the applications that they access, must log on using username and password once every ninety days which is enforced by the system.

3.4 For users that access Access Online CEE by entering a username and password, we will securely deliver the user's initial password to the designated user. The password is temporary and when first used the system will prompt the user to change it immediately.

3.5 Access Online CEE passwords must conform to the following password policy:

(a) Passwords should be between 6 and 32 characters long.

(b) Passwords are case–sensitive and should include at least one digit (0–9) and one character (a–z).

(c) Passwords may contain periods, commas, hyphens, etc.

(d) Passwords cannot contain more than 3 consecutive identical characters (e.g. 'aaaa' is not possible).

(e) Passwords cannot contain words from the user profile (e.g. user name, company, or city are not possible).

(f) Passwords will have to be changed at least every 90 days. Users will be notified seven days in advance.

(g) New passwords have to differ significantly from old passwords (a password history of twelve past passwords is retained).

3.6 All passwords are hashed (in other words, a "digital fingerprint" is created for each password).

3.7 A user has three attempts to enter the correct password, after which the user will be disabled and will require the assigned security manager to contact and request the Bank to unlock the blocked user account by contacting the Bank.

4 Authentication and electronic signatures using Digipass

4.1 Users must use a Digipass token and Username in order to authenticate their identity when logging on to Access Online CEE. This is done as follows:

(a) The user enters his or her username in the logon screen;

(b) Access Online CEE displays a six–digit challenge code onscreen;

(c) The user enters the six–digit challenge code on his or her Digipass, which generates a response code based on the challenge code;

(d) The user types the response code into the response box onscreen;

(e) Our server verifies whether the response code matches the username entered, and that the Digipass token used to generate the dynamic password is the Digipass assigned to that user; and

(f) If the response code is correct, the user is granted access to the Access Online CEE service.

4.2 In various applications, users must use a Digipass token and PIN code to generate an electronic signature, also known as a Message Authentication Code (MAC) to authorise and transmit instructions to us. The MAC is used to authenticate the sender of each instruction, and to protect the integrity of the each instruction while it is stored and processed within our systems. The MAC is created using an electronic key stored in a central security module and verified before processing takes place. This MAC implementation offers protection from tampering with the instruction since authentication would fail if even one character within the instruction were changed. The MAC is generated as follows:

(a) Access Online CEE displays a eight–digit challenge code (also known as a "hash") onscreen, based upon the data which the client is signing;

(b) The user enters the hash on his or her Digipass, which will generate a response code based on the hash;

(c) The user types the response code into the response box onscreen;

(d) Our server verifies whether the response code matches the username entered, and that the Digipass token used to generate the dynamic password is the Digipass assigned to that user; and

(e) If the response code is correct, the instruction is accepted for processing by us and the user is informed onscreen that the MAC was successful.

4.3 Digipass realises the authentication and MAC functions using the Triple DES algorithm.

4.4 Digipass PIN code format:

(a) The PIN code is a 4 character numeric code to protect the unauthorised use of the Digipass token. The user has three attempts to enter the correct PIN code, after which the Digipass will be locked.

(b) Upon commencing use of the system the user will be prompted to change the initial PIN code issued by us. This represents a further security measure as now only the user has access to the PIN number.

4.5 Managing Digipass tokens and PIN codes:

(a) It is the responsibility of the security manager to deliver a Digipass to each authorised user. The Digipass will **only** be activated when we receive a notification of the delivery of the Digipass and PIN to the end–user by the security manager.

(b) Each Digipass, with its unique PIN code is intended for the exclusive personal use by the assigned user. Accordingly, a Digipass must not be transferred, loaned, or shared, even if the other person has been authorised to submit instructions to us. Within the organisation, the security manager administers users who are authorised to use Digipass token.

(c) The user must exercise due care with the Digipass and PIN code issued to him or her.

5 Security during transmission

All data that Access Online CEE transmits is encrypted using 128–bit Secure Socket Layer (SSL) encryption, which maintains the confidentiality and integrity of the data while communicated over the Internet. SSL protocol establishes the identity of the web site and encrypts the transmission channel between web browser and web site to keep transmitted information confidential. Only the user who establishes a secure web connection can see the data unencrypted. Any attempted change to the data will be detected and disallowed.

6 Security at client location

6.1 As a PC is considered a non–secure software environment you must apply the following additional security measures to enhance the integrity of this environment:

(a) Installing PC security software packages, including anti–virus software

(b) Regular updates of anti–virus software and other security related software, including the operating system and browser.

(c) Periodical deletion of unneeded security certificates, which may be configured in the installed browser by default.

(d) Changing your Access Online CEE password every 90 days (when applicable).

To further enhance PC security, all users must be instructed to adhere to the following guidelines:

(e) Passwords or PIN codes must never be revealed to others.

(f) PCs must never be left unattended when Access Online CEE is running. Users leaving his or her desk for a short period must either logout from Access Online CEE, or use a password–protected screensaver.

7 Audit Trails

The Bank records audit trails for Access Online CEE:

7.1 for the Access Online CEE payment warehousing on user level where events are logged other critical functionality, such as the user authentication.

Schedule – BankOnline – UAE – Balance and Transaction Reporting module

1. BankOnline – Balance and Transaction Reporting module

The BankOnline – Balance and Transaction Reporting module, as further described in the user manuals will enable you to:

(a) Obtain information, including information on balances and transactions from the accounts;

(b) Deliver and receive information between us;

(c) View on screen images of cheques collected by us on your behalf; and

(d) Do any other transaction as we may permit under the BankOnline – Balance and Transaction Reporting modules from time to time.

2. Equipment

You are responsible for ensuring the compatibility of your Internet browser, its settings and any of your equipment with the BankOnline – Balance and Transaction Reporting module.

Schedule – OfficeNet/MultiCash

1 OfficeNet MultiCash™

OfficeNet/MultiCash™ as further described in the user manual will enable you to:

(a) transfer funds to and from the accounts;

(b) obtain information, including information on balances and transactions from the accounts;

(c) set up direct debit payments to be made from the accounts;

(d) set up collection orders to be made to the accounts;

(e) generate bank cheques from the accounts;

(f) deliver and receive information between us; and

(g) do any other transaction as we may permit under OfficeNet/MultiCash™ from time to time.

2 Our Obligations

2.1 We will:

(a) deliver the self–installing software to you or provide the necessary support to assist you to install the software; and

(b) provide training and support to you in relation to OfficeNet/MultiCash™, as agreed between us and you.

2.2 If you experience a malfunction with the software, you agree to immediately report the same to us in writing (using reasonable detail to describe the malfunction). For the avoidance of doubt, we will not repair computer hardware or other failures arising from your interference with the software. If computer hardware defects occur, you must ensure maintenance with your relevant supplier of the computer hardware.

3 Your Obligations

3.1 Where required by any law or directive of any state or organisation, you shall obtain all necessary consents, approvals, licences and permits from all authorised representatives, third parties, governmental agencies and regulatory authorities to any use or marketing of personal data and to the international transfer of personal data by us via the electronic banking service.

3.2 You agree that on our reasonable request you will provide us with copies of any such consent, approval, licence or permit.

4 Software Licence

4.1 In order to use OfficeNet/MultiCash™, you are granted a non–exclusive non–transferable licence to use the software on the following terms and conditions:

(a) you agree to only use the software for the purposes set out in clause 1 above;

(b) you will not copy, publish, sell, rent, lease, sub–license, distribute, loan, modify, merge, translate, decompile, reverse compile the software (or any part of it) or make any other use of the software except:

(i) as expressly permitted by law;

(ii) for making one copy for the purpose only of being used by you in lieu of the original copy in the event that the original copy is lost or rendered unusable; or

(iii) as agreed in writing by us;

(c) we reserve the right to upgrade the software. If you are provided with the upgraded software, you are obliged to install it on your equipment as soon as practicable and stop using the old software. Any upgrades will be made available to you on these terms and conditions;

(d) you will treat the software as confidential;

(e) except with our consent, you will only use the software for your own business purposes and not for the purpose of providing services for any third party;

(f) you will not make the software available to any third party;

(g) you will allow us, our affiliates, agents and our sub–contractors reasonable access to enable us to examine and test the software or to carry out any maintenance, improvements or new developments; and

(h) you will not do anything which would result in any infringement or unauthorised use of our or our suppliers' intellectual property rights in the software or the user manual.

4.2 For the avoidance of doubt, you will not acquire any title, ownership interest or intellectual property right in the software or the user manual.

4.3 We warrant that the software supplied by us to you provides in all material respects the functions set out in the user manual, provided it is properly used on the equipment and with the operating system for which it was designed, as set out in the user manual. So far as permitted by applicable law, we do not make any other warranty express or implied, statutory or otherwise, as to the condition, quality or performance or fitness for purpose of the software.

4.4 We will indemnify you against any loss you incur as a result of any legal action based on an allegation that the software infringes any intellectual property right of any third party provided that you:

(a) promptly inform us in writing (in reasonable detail) of the existence of any such legal action;

(b) make no admission of liability;

(c) do not reach any settlement; and

(d) leave the handling of the case entirely to us. For this purpose you agree to execute all documentation we reasonably request and provide us with all information and co–operation required to defend any such action. You also consent to us retaining the benefit of any such litigation.

4.5 You will be responsible for maintaining the security of your data and ensuring that your data is adequately backed–up. We will not be liable to you for the loss of your data in any circumstances regardless of whether such data is also maintained by us.

5 Equipment specification

5.1 You may only install the software on equipment which is compatible with the software and which meets the standard we have specified in the user manual.

5.2 You are responsible for ensuring the compatibility of any equipment with the software.

5.3 As a condition for the delivery of the software, you agree that you will provide the necessary phone line and hardware equipment with an installed and functioning operating system, as per our specifications and communication requirements.

6 Collection Orders

You agree to obtain all appropriate agreements before instructing us to set up any collection orders for payments to be made into your account. You agree that on our reasonable request you will provide us with copies of any such agreements.

7 Security

You will ensure that:

(a) all payment instruments and security tokens are held securely by you;

(b) all security tokens are only issued by your security personnel to your authorised representatives;

(c) all PIN numbers and other passwords are known only to your authorised representatives and are never recorded in any written form; and

(d) the software and related equipment are maintained in a suitably secure environment and are not left unattended while any third party is present.

8 Termination

The licence of the software to you is effective until you terminate it by destroying or deleting the software together with all copies. It will also terminate if the EBCs or your right to use OfficeNet/MultiCash™ is terminated or if you fail to abide by any of these terms and conditions, whether by an act or omission to act. Upon termination you must destroy or delete all copies of the software and the user manual, including any software stored on the hard disk of any computer under your control (or, if we request, return all copies to us).

Schedule – Online Client Service

1 Online Client Service

Online Client Service as further described in the user manual will enable you to:

(a) deliver a request to us seeking the resolution of any query you may have with any of our banking products or services (each such request a service request);

(b) obtain information from us on the status and progress of each service request received by us;

(c) obtain information from us, including information on balances and transactions relating to your accounts;

(d) obtain information from us on the products and services that we provide to you, and

(e) avail of any other service as we may permit under Online Client Service, from time to time.

2 Equipment

You are responsible for ensuring the compatibility of the Internet browser, its settings and any equipment with Online Client Service.